UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/425,736	10/22/1999	YUSAKU FUJII	991176	9951

38834 7590 05/04/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/425,736	FUJII ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/30/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) *2, 13* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-12, and 14-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/22/1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claims 1, 3-12, and 14-22 have been examined (Claims 2 and 13 have been cancelled).

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/30/2004 has been entered.

Response to Arguments

Applicant's arguments filed on 8/30/2004 have been fully considered but they are not persuasive. In response to applicant's argument that the cited prior arts Pare, Jr. et al. and Gressel relate to techniques for making the authentication demand by the personal ID and the organic information when the service is used in the service providing system of the present invention, where the present invention relates to the apparatus and method for detecting an illegal attacker who accesses the service providing system, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art. See *In re Casey*, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 312 F.2d 937, 939, 136 USPQ 458, 459 (CCPA 1963).

Examiner respectfully disagrees with applicant. Due to the manner of the claim language, major portions of the claims 1 and 12 still read upon the cited prior art Pare, Jr. et al. The claim language as presented does not differentiate the apparatus/method for an unauthorized member attempting to gain access to the system from detecting an illegal attacker who accesses the system.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 3-12, and 14-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1:

Claim 1 recites a "service providing system" as well as a "service providing apparatus" where the statutory class of a system and apparatus is the same. Thus, it is unclear whether the applicant intended to refer to the service providing system previously introduced in line 1 of the claim, or if the service providing apparatus differs from that one, in which case it is suggested that the applicant use another term in order to avoid confusion between the two. In order to further treat these claims on their merits, examiner interprets the service providing apparatus to be a portion of the service providing system, where the service providing system is presumed to be the system as a whole inclusive of each apparatus described.

Furthermore, it is unclear what a "use information storing unit" is. In order to further treat this claim on its merits, examiner presumes that this refers to a check to see whether or not someone has used the system before.

As per claims 3-11:

These claims recite "an apparatus according to claim 1" where it is unclear which apparatus (or maybe system) the applicant is referring to since there are multiple ones introduced. In order to further treat these claims on their merits, examiner interprets the apparatus to be referring to the overall system in general as declared in the preamble of claim 1.

As per claim 12:

Claim 12 recites the limitation "the apparatus" in line 6, where an apparatus has not previously been defined in this method claim. Also, claim 12 recites "said service providing apparatus" in line 8, where a service providing apparatus has not been previously introduced. Furthermore, there are other limitations in which this issue recurs. Thus, there is insufficient antecedent basis for these limitations in the claim. In order to further treat this claim on its merits, examiner interprets that applicant intended to refer to "the apparatus" as "an apparatus," "said service providing apparatus" as "a service providing apparatus," and the other limitations following the same scheme interpreting the/said to a/an depending on the specific limitation.

Furthermore, it is unclear what a "use information storing step" is. In order to further treat this claim on its merits, examiner presumes that this refers to a check to see whether or not someone has used the system before.

As per claims 14-22:

These claims are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 5, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pare, Jr. et al., United States Patent No. 6,581,042, and further in view of Subbiah et al., United States Patent No. 6,035,403.

As per claims 1 and 12:

Pare, Jr. et al. substantially teach a service providing system/method comprising: a service providing apparatus/method in which organic information of the user is previously registered in correspondence to ID information (col. 4, lines 9-13), ID information and organic information based on an authentication demand of the user are inputted, the registered organic information corresponding to the inputted ID information is read out and collated, and when they coincide, use of the apparatus is permitted (col. 4, lines 13-29 and col. 9 line 50 - col. 10 line 8); and an illegal access discriminating apparatus for discriminating an illegal attacker to said service providing apparatus/method, wherein access by an said illegal access discriminating apparatus/method comprises: an inputting unit for inputting the ID information and organic information based on the authentication demand which said service providing system received from the user (col. 4, lines 13-17), a use information storing unit for storing ID information and organic information based on the authentication demand which the service providing system received in the past from the user within a predetermined time (col. 9 lines 32-40, where the

"predetermined time" is ever before); a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with ID information and organic information stored which were inputted and not previously registered in the past (col. 9 line 66 - col. 10 line 8, where the reason a party was not identified merely implies that they were not previously registered); and a control unit for discriminating an authentication demand by the attacker on the basis of an output of said comparing and collating unit and notifying said service providing apparatus of it (col. 10, lines 2-8).

Not explicitly disclosed by Pare, Jr. et al. is a storing unit for temporarily storing the ID information and organic information based on the authentication demand which said service providing system received from the user. However, Subbiah et al. teach the system capturing the organic material which is bound to ID information which the user entered in order to be authenticated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system/method disclosed in Pare, Jr. et al. to have a storing unit for temporarily storing the ID and organic information supplied by the user upon an identification demand, where capturing[1] implies storing based on it's definition. Furthermore, since the storing unit would be storing the "temporary" form of the user ID and organic information entered, it would be obvious to only save this information temporarily, i.e. form the amount of time that the authentication process takes place for. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was

[1] According to the Cambridge Advanced Learner's Dictionary Online, the relevant possible definition of the term capture is pasted below:

verb [T]

3 to record or take a picture of something using a camera: *A passer-by captured the whole incident on film.*

6 SPECIALIZED If a computer or similar machine captures information, it takes it in and stores it.

made, would have been motivated to do so since it is suggested by Subbiah et al. in col. 5, lines 18-32 and col. 9, lines 20-30.

As per claim 5:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Furthermore, Pare, Jr. et al. teaches a payer enters a PIN code into the keypad, then transmits the biometric-PIN for identification along with the hardware code and identifies the payer using the biometric sample (col. 13, lines 66-67 and col. 14, lines 1-8).

III. Claims 3-4, 6-11, and 14-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pare, Jr. et al., United States Patent No. 6,581,042 and Subbiah et al., United States Patent No. 6,035,403 as applied to claims 1 and 12 above, and further in view of Gressel, United States Patent No. 6,311,272.

As per claim 3:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach control unit determines that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of the comparing and collating unit. Gressel teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized (col. 10, lines 26-34). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow unauthorized entries to be halted.

As per claim 4:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al, because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 6:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach the inputted organic information and the organic information which was inputted in the past coincide, the control unit detects a combination in which the organic information coincides and the ID information differs, and when the number, the control unit determines that there is the authentication demand by the illegal access person. Gressel teaches a false rejection rate rejects a percentage of individuals when the meeting of the two (false acceptance rate and false rejection rate) nears the threshold (col. 10, lines 5-23). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow the attempted user to be authenticated.

As per claim 7:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence and an organic information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained and generating a signal indicative of dissidence of the organic information in the case where a value less than the predetermined coincidence degree is obtained. Gressel teaches a percentage of the population would be rejected and the guards would be signaled (col. 10, lines 48-54). Also, Gressel teaches a false acceptance rate and false rejection rate (col. 9, lines 50-67) and upon comparison with the threshold value, a large subgroup would be allowed entry (col. 9, lines 50-67 and col. 10, lines 1-5). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow personal information to be used in records for authorization with a specific individual.

As per claim 8:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into

the smart card, the original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). 11: would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 9:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Furthermore, Pare, Jr. et al. teach an ID module conducts a re-registration check and comparing the registration biometric sample with other biometric samples (col. 9, lines 33-41). Pare, Jr. et al. and Subbiah et al. fail to teach the storing unit stores a telephone number serving as a transmitting source and a terminal position such as a network address or the like together with the ID information and organic information which were inputted in the past. Gressel teaches secret keys and random numbers are internally generated in smart cards and security application modules in terminal devices. Biometric data in a secure system is equivalent to pins and passwords. (col. 11, lines 47-57). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. to designate a personal ID as telephone numbers and biometric data to increase the security of the apparatus.

As per claim 10:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach an authentication demand terminal address recording unit for recording the number of times of authentication demand every terminal address and the same terminal access detecting unit for detecting that the authentication

demand of a predetermined number or more has been performed within a predetermined time with reference to the authentication demand terminal address, activating the comparing and collating unit and the control unit and allowing an illegal access to be discriminated. Gressel teaches the use of an original template threshold value, which sets values that are larger than the user's smart card threshold value. This threshold value is incremented appropriately and thus records the demands on the authentication process Gressel teaches the use of a biotest to compare fingerprints where only 3 percent of the population would be rejected (col. 12, lines 45-51). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because preliminary screening of users reduces fraudulent access to the authentication system, thus reducing processor time.

As per claim 11:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 1 above. Pare, Jr. et al. and Subbiah et al. fail to teach that when it is determined that there is the authentication demand by the illegal access person, the control unit automatically notifies an administrator of the service providing system of a result of the discrimination. Gressel teaches a rejection results in the further processing of the applicant by a guard (col. 10, lines 48-54). The guard is comparable to an administrator. It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because the use of an administrator's intervention would facilitate the accuracy of the authentication process.

As per claim 14:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach a control step, it is determined that

there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information does not coincide on the basis of the output in the comparing and collating step. Gressel teaches that 3% of the population would be rejected regardless of the value of the threshold. Human intervention then becomes necessary to process the applicant. (col. 10, lines 48-54) It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because of the need to resolve the authentication of applicants who qualify for access with a valid threshold value, but not qualifying organic information.

As per claim 15:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach telephone number serving as a transmitting source, a terminal position such as a network address, and an input time in correspondence to the ID information and organic information which were inputted in the past are stored and in the control step, it is determined that there is the authentication demand by the illegal access person in the case where the comparison result in the comparing and collating step between the inputted from a same terminal position within a predetermined time indicates dissidence. Gressel teaches secret keys and random numbers are internally generated in smart cards and security application modules in terminal devices. Biometric data in a secure system is equivalent to pins and passwords. (col. 11, lines 47-62). An original template resides in the terminal while a threshold value is in a user's smart card (col. 12, lines 46-51). 3% of the population would be rejected regardless of the value of the threshold. Human intervention then becomes necessary to process the applicant. (col., 10, lines 48-54) It would have been obvious to

combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. to designate a personal ID as telephone numbers and biometric data to increase the security of the apparatus, to store the information to use for authentication, and because of the need to resolve the authentication of applicants who qualify for access with a valid threshold value, but not qualifying organic information.

As per claim 16:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach past ID information has a serial number for the inputted ID information or not is discriminated and, when it is determined that the past ID information has the serial number, il: is determined that there is the authentication demand by the illegal access person at a predetermined designated number of times. Gressel teaches a fingerprint scan is used in a biotest scan, the threshold value has little effect on the test, and an illegal access person has a limited number of tries because of their fear of being caught (col. 10, lines 40-47). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because a biotest scan would deter unauthorized access attempts and minimize the authentication systems use of the processor.

As per claim 17:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach the inputted organic information and the organic information, which was inputted in the past coincide, a combination in which the organic information coincides and the ID information differs is detected, and when the number of the combinations reaches a predetermined number, it is determined that there is the

authentication demand by the illegal access person. Gressel teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized (col. 10, lines 26-47). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow unauthorized entries to be halted.

As per claim 18:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence and an organic information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained and generating a signal indicative of dissidence of the organic information in the case where a value less than the predetermined coincidence degree is obtained. Gressel teaches a percentage of the population would be rejected and the guards would be signaled (col. 10, lines 48-54). Also, Gressel teaches a false acceptance rate and false rejection rate (col. 9, lines 50-67) and upon comparison with the threshold value, a large subgroup would be allowed entry (col. 9, lines 50-67 and col. 10, lines 1-5). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow personal information to be used in records for authorization with a specific individual.

As per claim 19:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 20:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48) The ID module detects a payee or payor by conducting a re-registration check (col., 9, lines 33-41). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et

al. because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 21:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach an authentication demand terminal address recording unit for recording the number of times of authentication demand every terminal address and the same terminal access detecting unit for detecting that the authentication demand of a predetermined number or more has been performed within a predetermined time with reference to the authentication demand terminal address, activating the comparing and collating unit and the control unit and allowing an illegal access to be discriminated. Gressel teaches the use of an original template threshold value, which sets values that are larger than the user's smart card threshold value. This threshold value is incremented appropriately and thus records the demands on the authentication process. Gressel teaches the use of a biotest to compare fingerprints where only 3 percent of the population would be rejected (col. 12, lines 45-51). It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because preliminary screening of users reduces fraudulent access to the authentication system, thus reducing processor time.

As per claim 22:

Pare, Jr. et al. and Subbiah et al. substantially teach the system/method as applied to claim 12 above. Pare, Jr. et al. and Subbiah et al. fail to teach that when it is determined that there is the authentication demand by the illegal access person, the control unit automatically notifies an administrator of the service providing system of a result of the discrimination. Gressel

teaches a rejection results in the further processing of the applicant by a guard (col. 10, lines 48-54). The guard is comparable to an administrator. It would have been obvious to combine Gressel's teachings to Pare, Jr. et al. and Subbiah et al. because the use of an administrator's intervention would facilitate the accuracy of the authentication process.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2133
4/19/2005

NK

GUY LAMARRE
PRIMARY EXAMINER